FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

IMPROVEMENTS IN AND RELATING TO ACCESS CONTROL

Field of the Invention

The present invention relates to access control devices and methods.

Background to the Invention

Password protection is often used to control access to data or software as a result of which considerable attention has been paid to the breaking of password protection.

Referring to Figure 1 of the drawings that follow, there is shown a representative flow diagram of a prior art password protection method, according to which a corresponding device operates. In the Figures the abbreviation "PW" is used for "password".

At 100 a selected password is entered. The password may be user-selected or allocated in some other way.

The selected password is stored (102) at a memory location within the device. The device then enters its normal operation (104) as part of which it determines as each access request is submitted whether this is a password protected access (106). If it is not a password protected access, the "NO" branch is followed and normal operation resumes. If it is a password protected access, the "YES" branch is followed and a password is requested (108). Upon input of a password, the input password is compared (110) with the password stored at a memory location. If the

input password is the same as the stored password (112) the "YES" branch is followed and normal operation resumes (104). Otherwise, the "NO" branch is followed and access is denied (114). As is well known in the art, instead of denying access upon the first input of an erroneous password, a further try or several further tries may be permitted up to a predetermined number of attempts with an incremented tamper count upon each failed password entry. In addition to denying access, alerts or alarms may be activated.

In the method and corresponding device described above, since the usual implementation is upon a digital computer, a de-bug program can be run alongside the password protection. As part of which, the de-bug program can, upon entry of any password, follow the program to the memory location at which the correct password is stored for comparison purposes. The de-bug program can then be used to copy the stored password from that memory location for correct entry. In this way, the prior art method and corresponding device described above is vulnerable to attack and to the bypass of the password security even if the data is encrypted.

It is an aim of preferred embodiments of the present invention to obviate or overcome at least one disadvantage encountered in relation to the prior art, whether referred to herein or otherwise.

Summary of the Invention

According to the present invention in a first aspect there is provided an access control device comprising means

for receiving an input password, means for combining the input password with a pre-selected code thereby to produce a combined password, and means for decrypting encrypted code using the combined password.

Suitably, the apparatus further comprises means for encrypting the combined password and the encrypted combined password is used for decryption.

According to the present invention in a second aspect, there is provided a method of controlling access, which method comprises the steps of receiving an input password, combining the input password with a predetermined code to produce a combined password, and decrypting encrypted code using the combined password.

Suitably, the combined password is encrypted and the encrypted combined password is used for decrypting encrypted code.

Suitably, the encrypted combined password is a key for decryption of the encrypted code.

Suitably, the password is an alphanumeric string. Suitably, the code is an alphanumeric string.

Suitably, the pre-stored access password comprises a pre-selected password combined with the predetermined code, which combination is encrypted.

Normally the combined pre-selected password is encrypted according to the encryption algorithm used for the combined password. Suitably, the encryption is

substantially unreversible (asymmetric). Typically, the encryption algorithm will be a public key algorithm.

According to the present invention in a third aspect; there is provided a computer program for executing the method of the second aspect of the invention.

According to the present invention in a fourth aspect, there is provided a carrier comprising a computer program according to the third aspect of the invention.

Brief Description of the Figures

The present invention will now be described, by way of example only, with reference to the drawings that follow; in which:

Figure 1 is a representative flow diagram of a prior art access control method.

Figure 2 is a representative functional flow diagram of an access control method according to the present invention.

Description of the Preferred Embodiments

Referring to Figure 2 of the drawings that follow, there is shown a flow diagram illustrating a method according to the present invention, according to which method a corresponding device may operate.

At (200) a password is selected. As with the prior device and method, the password may be user-selected or chosen in some other way.

The selected password is then combined with (202) with a longer password string at pre-selected locations therewithin. This produces a combined password which is encoded (204). Normally, the encoding step will comprise a public key, substantially irreversible, encryption, but in theory could be as simple as carrying out an AND or XOR operation.

The encrypted combined password is used as an encryption key to encrypt data (206) which may be software. Notably, the encrypted combined password is not stored in any memory location. Following this the device enters normal operation (208) as part of which it checks (210) whether a requested data/software access is password protected. If the access is not password protected the "NO" branch is followed back to normal operation. Otherwise, the "YES" branch is followed and a request is made for a password to be input (212). Upon input of a password, it is inserted into pre-selected locations of the predetermined string (214). This is the same predetermined string with which the original password is combined (202). This produces a combined password which is encrypted at (216) using the same encryption as at (204).

The encrypted combined password is used as a decryption key to decrypt the encrypted data/software to which access is sought. Therefore only entry of a correct password will properly decrypt the data/software.

By way of example, therefore, at step (200), the password "FRED" may be entered by a user. The selected password is combined with the string A7BX2Q66FEAR3YD at locations subsequent to characters 2, 6, 9 and 13 (by order). This produces (202) the following combined result: A7FBXS2RQ66EFEARD3YD. The underlined letters are the password letters inserted at pre-selected points within the longer string. They are underlined for the purposes of explanation only.

At step (204), the combined password is encrypted according to any encryption method. Preferably, a public key encryption is used but this need not be the case. This may result in an output as follows: 3XTAV2?8BAD99X. The encrypted result need not be the same length as the combined password. The encrypted combined password is then used as an encryption key to encrypt data or software. If password protected access is sought (210), an input password is requested (212). Here, if an incorrect password is entered, for instance "MOUSE" it will be combined (214) with the pre-selected string at the pre-selected locations to give the following result A7MBXS2QQ66UFEARS3YED. This combined input password is then encrypted (216) according to the same encryption used at step (204) and used as a decryption key to decrypt the encrypted data. As the key is wrong the decryption will be inaccurate.

In the case of the correct password "FRED" being input at (212), it will be inserted at corresponding locations encrypted and will correspond to the key used for encryption. Thus when used as a decryption key it will accurately decrypt the data.

Accordingly, neither the password to be used by the user nor the decryption key is not stored anywhere within the device. Thus, by inspection of the device running a for instance, de-bug program, an unauthorised user would not be able to gain access to the necessary password nor to the decryption key.

Although reference is made herein to "passwords" it will be appreciated that this could be any signal or combination of signals and need not be a word at all.

A device operating as set out above with reference to preferred embodiments of the invention may be embodied in computer software in a digital computer or otherwise, for instance on a carrier such as a floppy disk, compact disk or hard drive.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

Claims

1. An access control device comprising means for receiving an input password, means for combining the input password with a pre-selected code thereby to produce a combined password, and means for decrypting encrypted code using the combined password.

2. An access control device according to claim 1, in which the apparatus further comprises means for encrypting the combined password and the encrypted combined password is used for decryption.

3. A method of controlling access, which method comprises the steps of receiving an input password, combining the input password with a predetermined code to produce a combined password, and decrypting encrypted code using the combined password.

4. A method of controlling access according to claim 3, in which the combined password is encrypted and the encrypted combined password is used for decrypting encrypted code.

5. A method of controlling access according to claim 3 or claim 4, in which the encrypted combined password is a key for decryption of the encrypted code.

6. A method of controlling access according to any one of claims 3 to 5, in which the password is an alphanumeric string.

7. A method of controlling access according to claim 6, in which the code is an alphanumeric string.

8. A method of controlling access according to any preceding claim, in which the pre-stored access password comprises a pre-selected password combined with the predetermined code, which combination is encrypted.

9. A method of controlling access according to claim 8, in which the combined pre-selected password is encrypted according to the encryption algorithm used for the combined password.

10. A method of controlling access according to claim 9, in which the encryption is substantially unreversible (asymmetric).

11. A method of controlling access according to claim 10, in which the encryption algorithm will be a public key algorithm.

12. A computer program for carrying out the method of any one of claims 3 to 11.

13. A carrier comprising a computer program according to claim 12.

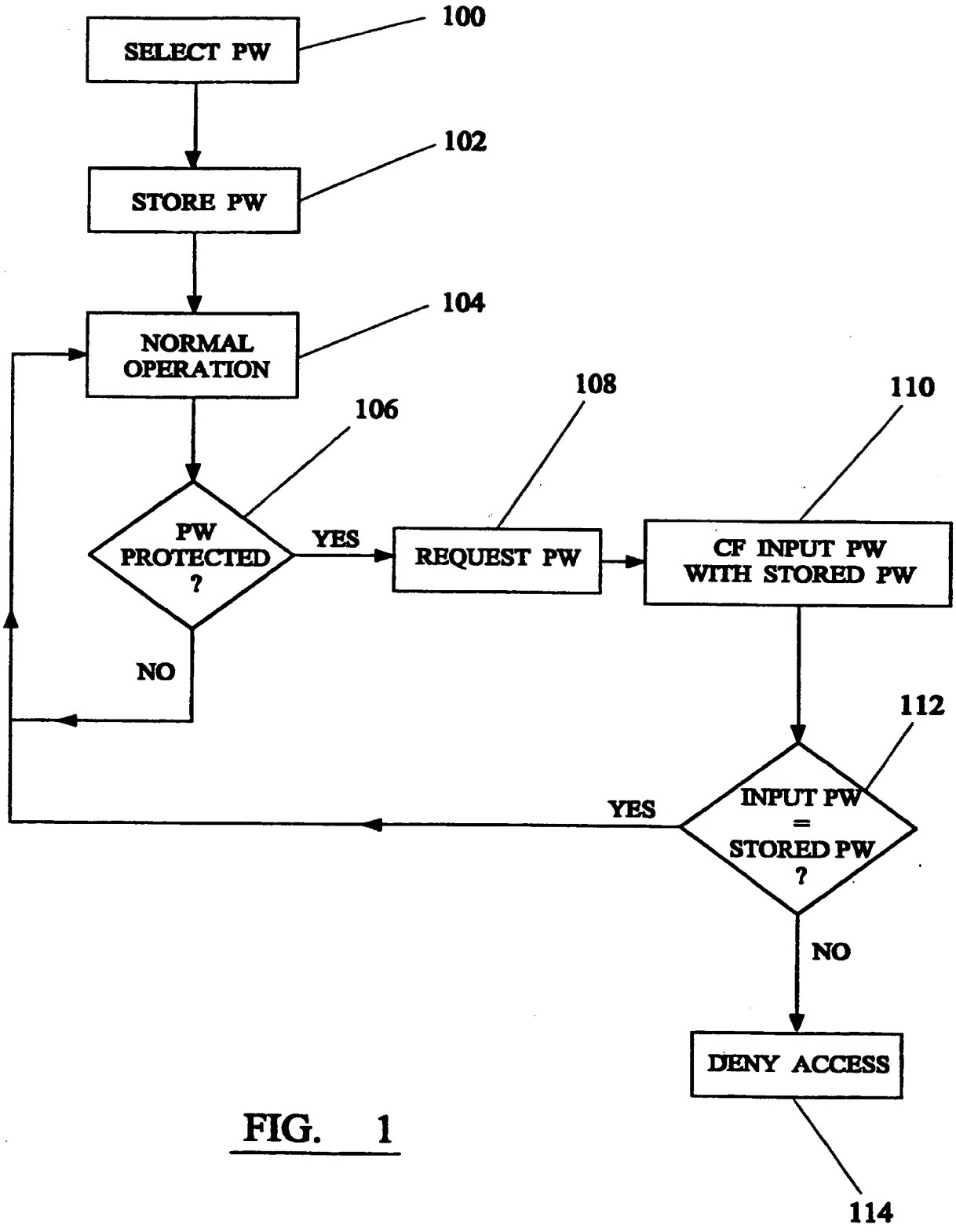
SELECT PW
100
STORE PW
102
NORMAL OPERATION
104
PW PROTECTED ?
106
YES
REQUEST PW
108
CF INPUT PW WITH STORED PW
110
NO
INPUT PW = STORED PW ?
112
YES
NO
DENY ACCESS
114

FIG. 1

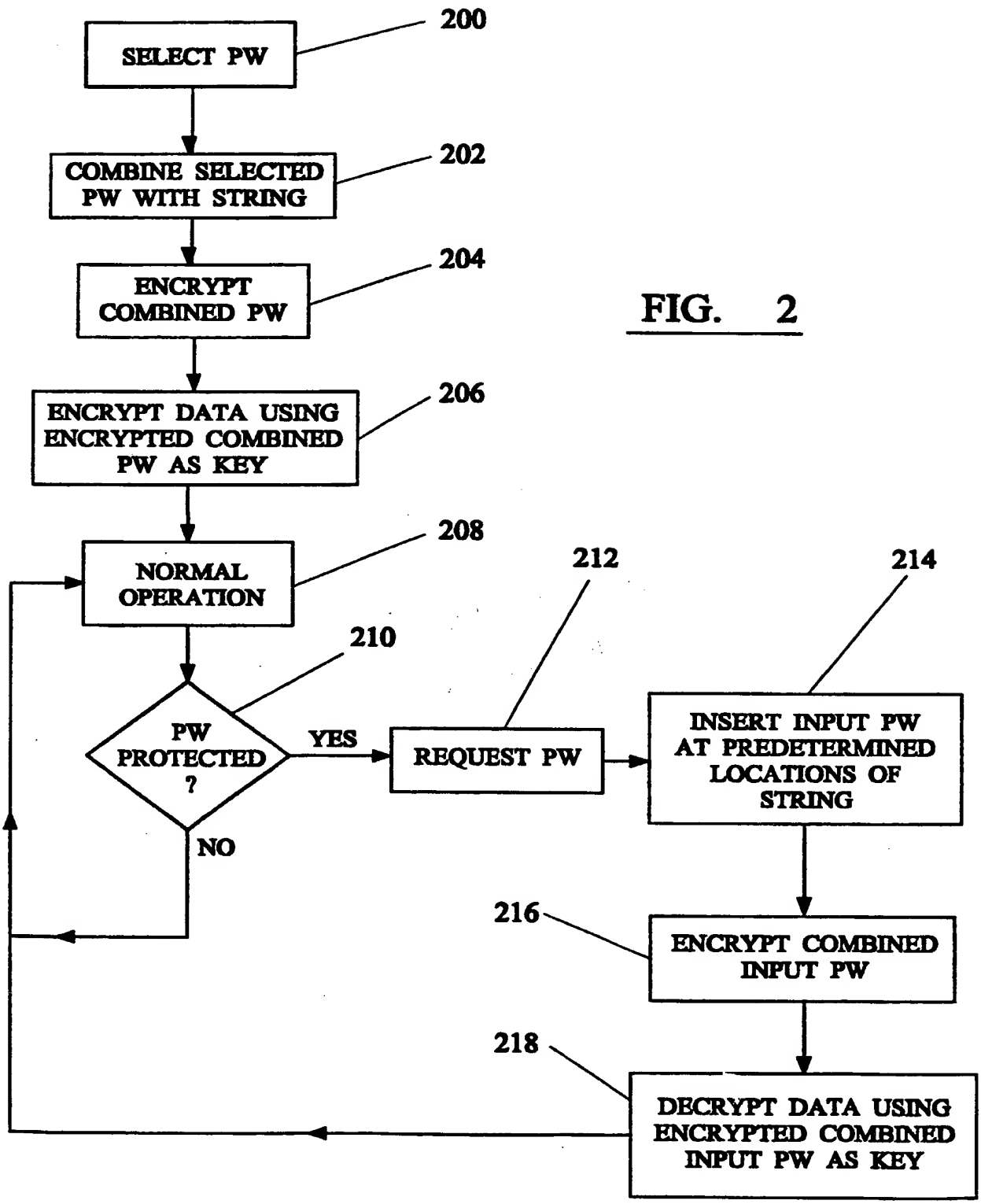
SELECT PW
200
COMBINE SELECTED PW WITH STRING
202
ENCRYPT COMBINED PW
204
ENCRYPT DATA USING ENCRYPTED COMBINED PW AS KEY
206
NORMAL OPERATION
208
PW PROTECTED ?
210
YES
NO
REQUEST PW
212
INSERT INPUT PW AT PREDETERMINED LOCATIONS OF STRING
214
ENCRYPT COMBINED INPUT PW
216
DECRYPT DATA USING ENCRYPTED COMBINED INPUT PW AS KEY
218

FIG. 2

INTERNATIONAL SEARCH REPORT

onal Application No
PCT/GB 99/02673

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 768 373 A (GRAWROCK DAVID ET AL) 16 June 1998 (1998-06-16) the whole document	1-13
A	US 5 677 952 A (ROGAWAY PHILLIP W ET AL) 14 October 1997 (1997-10-14) abstract; figure 3 claim 20	12,13
A	US 5 485 519 A (WEISS KENNETH P) 16 January 1996 (1996-01-16) the whole document	1-13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 December 1999	10/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...nation on patent family members

...onal Application No
PCT/GB 99/02673

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5768373 A	16-06-1998	EP 0894377 A	03-02-1999
		WO 9742732 A	13-11-1997
US 5677952 A	14-10-1997	US 5454039 A	26-09-1995
		EP 0658022 A	14-06-1995
		JP 7199808 A	04-08-1995
		SG 44363 A	19-12-1997
		US 5675652 A	07-10-1997
		US 5835597 A	10-11-1998
US 5485519 A	16-01-1996	US 5367572 A	22-11-1994
		US 5237614 A	17-08-1993
		US 5657388 A	12-08-1997
		US 5479512 A	26-12-1995